4/9/80

Science and Technology Advisory Panel

Dear Stan,

This document discusses in greater detail certain of the points about SAFE raised with you during the STAP meeting on Friday, 14 March 80; included are options we believe to be workable and recommend for your consideration.

Needless to say, the undersigned and the rest of STAP would be anxious to provide any further support you might seek in more extended explorations of these points.

[redacted]
Chairman

STATINTL

[redacted]

STATINTL

Encl - [redacted]

STATINTL

Options for SAFE

A Report of the DCI's
Science and Technology Advisory Panel

STIC 80-002
April 1980

Contents

STAP OPTIONS FOR SAFE

1. Introduction

On 18 March 1980 we forwarded to you eight questions regarding the future evolution of the SAFE system and the relation of CIA SAFE to other community systems (See Appendix I). In this report we propose various actions which, if implemented, could yield a more valuable community asset in the long run. Because of the size of the system and its complexity, a delay (6 months to two years) in IOC can be anticipated. Productive use of this delay time can be made, as we discuss in subsequent sections.

In our examination of SAFE, we were impressed with the need for a community manager of the ADP-communication systems. None now exists and SAFE is not being integrated into an overall community architecture. As a result the incremental value of SAFE will be less than it could be. Even without a community manager, the future capabilities of SAFE could be strengthened and possible steps in that direction are described in Section 2. The longer term questions of technical direction of the overall Intelligence Community ADP-communication systems will be the subject of additional STAP analysis and should be considered a separate issue from that of SAFE.

The evolutionary development of SAFE will require analysis of how the community uses SAFE. Sections 3 and 4 describe means by which such analysis could proceed. As SAFE comes on line, it will be essential for future planning to evaluate its usefulness. A possible means for evaluation is described in Section 5.

Finally, we believe that a rich body of experience in systems similar to SAFE exists and could be beneficially applied to enhancing SAFE's capabilities. To this end, we

propose in Section 6 establishment of an Advisory Council on Technology for SAFE.

This report primarily examines CIA SAFE and its use by the Intelligence Community. Our emphasis on CIA SAFE derives from the fact that NFAC stands to benefit greatly from a truly operational SAFE. DIA needs center on the accuracy, maintenance capability and general utility of their large encyclopedic files. These files require restructuring and improved maintenance capability as well as a high level of concurrency in use. Our analysis focuses on the analyst support function of SAFE; this function is of secondary importance to DIA. DIA's requirement can more easily be met than CIA's. Thus while we propose a "true pilot SAFE" for CIA, such an activity should not impede the development of the DIA SAFE. Indeed, the lessons learned in the "true pilot SAFE" will be of use in the evolutionary development of the DIA system.

In outlining the options for the future, we are fully aware of and appreciate the concerns of the SAFE management office and the Office of Central Reference. The steps outlined below will delay the scheduled delivery of an operational system, but we believe that the present schedule cannot be met since such critical items as command language and central hardware have not yet been decided upon. The delay we anticipate can be put to use to obtain operational experience on a "true pilot SAFE." The delays whether anticipated or not will cause problems with OMB and Congress and these should be recognized now.

2. Strengthening the SAFE Management

Strengthening of the community management of SAFE is essential if it is to become effective in satisfying its prescribed functions, and be capable of expanding flexibly and responsibly to aid the entire community.

The fundamental component of such strengthening must be increased technological awareness and capability at the appropriate managerial echelon. It is vital that decisions that affect the future performance of a large part of the community not be made by default by those who do not exercise the corresponding responsibility. Such decisions should not be delegated either to lower echelons or to contractors.

The context of SAFE is a large and intimidating R&D effort. Technical decisions must be made amidst both aggressive contractor actions and critical ongoing operational tasks. These decisions may commit the community far beyond the decisionmaker's ken.

Management itself, as an abstract entity, must be able to deploy experience and judgment in the following areas, at least:

1) Intelligence Production
   a) Collection
   b) Processing
   c) Storage and retrieval
   d) Analysis
   e) Output and distribution

2) Analytic processes: Some experience and grasp in substantive areas of intelligence; that is, economic, political, military, or S&T.

3) Technology and R&D for Intelligence
   a) Information sciences
   b) Communications
   c) Computer technology

4) Management and Human Factors

Whatever the particular details of the management structure, it is clear that experience and decisionmaking capacity must be accompanied by the appropriate authority--that requires rank and status to match the control to be exercised.

Given the ongoing function of intelligence production, Technology and R&D (number 3) is the most difficult area to fill, because it has been and is changing so fast.

Nevertheless, it is vital to fill it, for otherwise most of the important decisions about SAFE will be made without considering the potential for technological growth or possible technical constraints.

Delegation is always necessary in any large management task, but the overall management responsibility cannot be delegated away. If the managers cannot themselves be technologically knowledgeable enough to monitor the technological decisions about design and performance, they must establish a mechanism to ensure that decisions are adequately monitored and verified.

There are several possible ways of doing that:

1) Hire, beg, or borrow deputies with the needed competencies.

2) Borrow consulting as needed from other operating offices in the community. A problem with this is that loyalties and motivation will almost surely be at best divided.

3) Establish a continuing Advisory Council on Technology (ACT), combining in-house and outside experts. This is useful chiefly for guidance on the most important decisions, and for monitoring directions and performance.

4) Establish similar Ad Hoc Panels for particular important decisions. Such panels must invest a lot of time becoming aware of the context of the problem, so their cost-effectiveness will be low on the average. Furthermore, they cannot perform the monitoring function. They may be essential in crises or surprise contingencies.

5) Establish a responsive contractor management scheme. It is hard for contractors to understand deeply the desiderata that obtain for a system like SAFE, for integration with the most profound processes of intelligence production.

On a project as crucial as SAFE, we recommend number 1 above, coupled with number 3. Deputies with full technological competence are probably essential, if only to

provide full-time support with undivided loyalties. They must, of course, have the rank and authority to deal with their contractor counterparts.

It is also likely that some outside expert advice would be helpful; and for 3) above, a standing Advisory Council on Technology (ACT) would seem most fitting. It is not clear whether the council should restrict its considerations to SAFE, or should in fact ultimately deal with a broader range of technological problems. These questions are amplified below in Section 6.

3. A True Pilot SAFE

Interim SAFE was initiated in 1974 as a set of capabilities on a 370/158 run by ODP. Four main capabilities were sought for the original SAFE project, and they are still valid today:

1) A mail/message/distribution system

2) Private files available on-line for analysts

3) Public files available on-line for analysts

4) On-line facilities for read, edit, write, and document production

These four have to be somewhat extended and modified in detail to match either today's purported goals or the real needs that underlie the requirements for the system.

The chief uses made of interim SAFE were:

1) To provide limited experience for certain analysts in order to survey their expressed needs.

2) To demonstrate the capabilities to management echelons, in order to help with the budget and funding processes.

3) To derive certain specifications that might serve as guides for the actual SAFE system specifications.

4) To illustrate the capabilities in the intelligence environment to possible proposed SAFE contractors.

It is important to observe that Interim SAFE was never used as a pilot system as that term is used in engineering--that is, to provide experience with a small system whose performance is operationally projected to be what the final system ought to be. In practice, of course, the pilot system serves in engineering to modify requirements and specifications in both usage and engineering.

In Interim SAFE, we were informed that in general statistics about usage were not gathered because they would be "not representative."

The questions that ought to be answered by a true pilot SAFE include:

1) What are the usage patterns of naive users?

2) What are the usage patterns of experienced users?

3) What needs for modifications of SAFE performance become manifest from the transition of naive users to experienced ones?

4) What are the user documentation and training requirements?

5) What new requirements emerge from the experienced usage?

6) How should the services provided by SAFE be modified to take advantage of new technology?*

7) What facets of the system can be safely frozen in design concept? What parts must be carefully engineered to retain flexibility of function and performance?

Only a few of these questions can be dealt with through the current Interim SAFE. But there has been a great deal of experience elsewhere in systems similar in nature and size to SAFE; we note the unique aspects of much of the intelligence environment, which is why a true pilot SAFE is needed. But if advantage is taken of the continuing experience of these other systems, it is likely that the process of initiating a pilot SAFE and interacting with it to guide final SAFE development can be speeded up.

The questions above that seem at first glance to be uniquely answerable by pilot SAFE are 1, 2, 3, and 5. These have to do with analyst usage of the tools and capabilities provided to them. We are therefore suggesting that a first step is to start collecting systematic longitudinal data on analyst usage of the current Interim SAFE, continuing during a conversion to a true pilot SAFE.

There is little doubt that the general capabilities sought can be provided on a small scale by any of a large number of current installations outside the community, as well as inside. At least four members of STAP have had wide experience with such systems. Such systems also provide some of the extra capabilities that are not now planned as part of SAFE, but that are considered highly desirable, including:

1) collaborative capabilities, whereby several analysts can simultaneously and remotely collaborate on the same task.

---

*For example, good split-screen graphics terminals can take advantage of more powerful editing capabilities than previous terminals.

2) general communications access to remote files over community or common carrier lines; this is relevant to making SAFE truly a community-wide resource, as is being strongly urged by certain members of the IC staff.

3) new evolutionary user languages, including the capability for user on-line control of multiple jobs simultaneously.

The actual implementation of pilot SAFE can therefore be handled in several ways:

1) Use the interim SAFE now running in ODP. Upgrade its capabilities, installing the above desired new capabilities, aiming at an integrated single system for continuing development.

2) Use an existing system from outside, but installed at the CIA, using outside contractor support as well as in house personnel.

3) Use an existing system at an outside contractor's installation, sending analysts on TDY to provide the usage, etc. The difficulties involved in this option are obvious, and it is included only for the sake of completeness.

The advantages of the first option are that interim SAFE is now running here, that both users and system personnel are familiar with it, and that it performs some of the needed capabilities already in the desired intelligence environment. The disadvantages are that some system reprogramming will be necessary to bring it to state of the art, and that this will likely need system architecture and programming resources beyond what is available here.

The advantage of the second option is that such a pilot system is nearly an off-the-shelf item, and could be running in the CIA fairly quickly. On the other hand, the special requirements of the community environment would enormously delay the user population as well as the systems and programming personnel at the CIA.

In summary, we strongly suggest option 1, i.e., use the current interim SAFE. A conscientious effort toward the kind of pilot SAFE being discussed here entails:

1) Increased technological resources available in house. This should include some contractor (TRW) personnel, plus some non-TRW contractor personnel, to keep the former honest, as it were. A total of six people for the first eight months would be needed, and then perhaps dropping to four on a continuing basis.

2) Enlarging the user population and the user studies. This is so important, and has so many ramifications, that is the subject of a separate Section 4.

3) Establishing a direct COINS link that will enable study and experimentation by analysts in community-wide access and retrieval.

4) Initiating data gathering and analysis of usage pattern and changes in usage patterns by analyst users (see also Section 5)

5) Testing prepared user languages and other tools as soon as possible.

No.

4. The Users of SAFE

There are two main reasons why the population of users of Pilot SAFE must be enlarged and modified from that of users of Intermim SAFE:

1) We need to find out answers to what users do, how they do it, and how they change.

2) We need users to find out what SAFE can do for them, and how it can be responsive to their developing needs.

The first dictates the initiation of the continuing study of user patterns of usage that we have already mentioned. An IBM study of a somewhat different user community illustrates the approaches and the attacks that might be considered; it

is included here as Appendix II. Beyond that, there are a number of points that are very hard to pin down, for they deal with finding out the unexpected: What new requirements will users make as they become experienced? Every large system has felt the impact of such phenomena. Indeed, part of the responsibility of management should be to make sure that evolving needs, even if they are poorly expressed or dimly felt, can be recognized, evaluated, and fulfilled.

In the beginnings of large scale computer utilization, computer users submitted jobs to the computer center, which responded with output, usually within hours, and sometimes days. The case for interactive use of computers was made very strongly in the 60s. It was mistitled time-sharing, but the real impact was the rapid response and control that it provided the user. What it means for the Intelligence Community is that the analyst can not only get output fast, but can also guide the processing and retrievals so as to satisfy requirements that may be hard to specify ahead of time. Many computer programmers, especially beginners, enjoy the actual process of interaction with a responsive computer; but in fact the interaction is valuable only as it cuts down the amount of time needed to specify what has to be done--that is, to cut down on the amount of interaction itself. How to do that depends very largely indeed on the habits and cognitive styles of the computer users, the analysts. That is one reason why close study of them and their practices will pay such big dividends.

The second need is of course at least partly bureaucratic. The users in the community are busy in the ways that they have diligently discovered serve them and their task the best. If we expect them to change their ways, we have to persuade them that it will be in their best self-interest to do so. To do that, we must make sure that there are visible and successful new users in the fields that we hope to serve. It is not useful to tell a political analyst that it will pay him to use a computer by showing him how a weapons analyst can deal with signal processing of radar data links. The user population should be carefully expanded, with users who will help, both in providing convincing evidence about the value of SAFE and also in participating in the development of the capabilities it can give. It is also necessary to pick important problems to solve using SAFE.

5. The Methodology of Evaluation

It will be clear from all the above that there is a great lack in what we know about specifying how we want SAFE to behave. As has been said, we need to know not only what analysts do now, but how they behave interactively with SAFE during and after substantial experience with it.

Further, although a first step is obviously to observe, record, and analyze patterns of usage by analysts, we reiterate* the urgency for a very general human factors study of intelligence analysis and the behavior of intelligence analysts. That is, we must construct a conceptual model of how an analyst reasons about his problems, as well as merely how he gathers the statistics discussed in earlier sections. SAFE can be made operational without it, but it will never be its most effective without such understanding. Nor can any other analytical methodology.

One of the underlying drives that leads to expression of a need is that of being able to evaluate the effectiveness of some change in organization, procedure, or personnel. But, if we have only a broad and unstructured estimate of effectiveness, it is difficult to determine whether a change in that estimate is due to previous decisions about organization and so on, or to the changing tides of the world crises.

The community needs to be able to tell more than that SAFE works, but also that it is cost-effective to such and such a degree, and in such and such respects. If we do not know that, we will not be able to assign resources efficiently to correct errors, add improvements and capabilities, and modify performance to meet changing requirements.

---

*This point has been made many times already; STAP has discussed it in a previous report, and one of the present authors (OGS) stressed it 4 years ago in a contract report to ORD's Center for the Development of Analytical Methodologies (CDAM).

So we need to know what analysts do as part of the intelligence process - the fundamental part, for it is the gem for which all the rest of the intelligence handling is but the setting and the supporting framework. The critical problem of evaluation is to determine and quantify the contributions to the overall system operation of every piece of the operating hierarchy.

This galaxy of problems - included in the term Methodology of Evaluation - has widespread ramifications. Besides needing to know whether a modification of SAFE is cost-effective or not, we need to know how to produce requirements for training SAFE users. Indeed, this is but part of a larger requirement for being able to evaluate training for the community as a whole.

The political and social complications from such studies should not be neglected, but they are certainly not reasons for delaying them. We believe that most analysts would welcome study of their behavior in producing intelligence analysis. Similarly, it is important, as we have emphasized in the Analytical Methodologies report, to be sensitive to the efficiency of current analytic practices in their current context, so that we can properly aid in the transitions to a more computerized context.

The logical base for these studies is ORD's Analytical Methodology Research Division. Some of these studies can be carried out totally in-house, but some will probably need some contracted assistance. The studies needed can be summarized:

1) Pilot SAFE usage studies: some questions were listed in Section 3. They should be extended with:

   a) Error and complaint log, with respect to system failures, new capabilities, inadequacies, documentation, etc.

   b) Special examination of usage by SAFE analysts of systems and files outside the CIA.

2) Other Human Factor Studies

a) Analyst access to non-computerized files

b) Analyst-analyst interaction in the production of intelligence output

c) The types and efficiencies of motivation for intelligence analysts

d) Models of intelligence analysts and the analytic process

3) Evaluation techniques developed for application to [as we discussed in the STAP Analytical Methodologies report.]:

a) Intelligence products

b) Intelligence analysts

c) Intelligence analysis

6. An Advisory Council on Technology

We have suggested that project SAFE management could benefit from an Advisory Council on Technology (ACT). Here we discuss the detailed duties and responsibilities of such a council, who might be the personnel and how it might be operated. We defer a suggestion that the council deal with the larger problems of technology in the entire community: because, first, SAFE is difficult enough; second, it will serve a community function, even though just the CIA and the DIA are involved initially; and third, such a responsibility can be more clearly defined after the ACT has proved its worth with SAFE.

The ACT would be a continuing body, comprising both community and outside personnel. The primary duty would be to assist the SAFE management. In detail, where so tasked, ACT should:

1) Make recommendations about major decisions concerning technology, new directions, and user-system interactions.

2) Make evaluations of past decisions as to their effect on SAFE operations, intelligence production, and future developments in technological applications.

3) Provide cost-benefit analyses for proposed changes or extensions to the SAFE capabilities.

4) Monitor certain variables, like interagency usage, or contractor performance on particular subtasks.

5) Provide a continuing link with the technological state-of-the-art.

6) Act as a sounding board, to responsively assist the SAFE management in creating long-range future plans.

Such functions cannot be satisfactorily performed by a group meeting quarterly. It is the monitoring functions that are crucial in demanding quick response from the group--how should they alert the management that coordination or redirection is needed quickly?

We believe that SAFE, or a system with SAFE like capabilities, is such a central part of the future intelligence processing of this country, that it is vital for its supporting management to represent the best that the community and the technology can afford. In the crucial transitions and developments that lie immediately ahead, continuity should also be maintained with the cognizant supervisory and review groups. Furthermore, any group like our suggested ACT must be perceived as working in support of the people who have the in-house responsibilities for SAFE.

In view of the current needs, the ACT should be prepared to exercise both review and monitoring functions with some intensity for the next few months especially. The most immediate duty must be to advise the DCI and SAFE management about the design review and possible acceptance this summer. As you know, we are of the opinion that this ought to be delayed or modified, and it is vital that the community

understand and support the decisions that will be made. In order to do that efficiently, the ACT should integrate the current projections by SAFE personnel about analyst usage in the future with the experience gained by outside efforts, as discussed in previous sections.

We therefore suggest that the ACT review some of the comparable outside systems mentioned above, together with appropriate personnel from SAFE itself. Such reviews should not be cursory; we would hope that the group could spend a minimum of three days at each installation, and possibly a working week, so as to receive not only system understanding, but also detailed user experience. It is important also for the group to receive views about the history and development of each system, in order to be able to apply the lessons learned to the community task.